

REMARKS

Favorable reconsideration and allowance of the present application are respectfully requested in view of the following remarks. Claims 1-3 and 45-78 are pending, and non-elected claims 56-78 are withdrawn from consideration. Of the pending claims, claims 1 and 47 are independent.

ALLOWABLE SUBJECT MATTER

Applicants appreciate for the Examiner's indication that claims 52-55 include allowable subject matter.

§ 103 REJECTION – SCHNECK, ISHIGURO, CONVENTIONAL ART

Claims 1-3 and 47-49 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneck et al. (USP 5,933,498) in view of Ishiguro (EP 874300 A2) and in further view of the conventional art described in the specification. Applicants respectfully traverse.

Regarding independent claims 1 and 47, the Examiner relies upon Figure 8, column 15, lines 19-38 and Figures 9-12, column 14, lines 32-50 of Schneck to allegedly teach the features of “a data storage medium for storing the digital data file transferred from a source device, the digital data file having been encrypted by: ... 1) generating a key data using at least a unique ID of the digital data playing device or a unique ID of the storage medium or both ... 3)

encrypting within the source device the digital data file using said key data.”

The Examiner provides no indication whatsoever regarding what he considers in Schneck to be equivalent to the recited features of the claims. For example, the Examiner provides no indication of how the data storage medium, the digital data playing device, the unique ID of the digital data playing device, the source device and the key data as recited in claim 1 read on Schneck.

Figure 8 of Schneck only discloses an access mechanism 114, which allows a user to access the data in the packaged data 108 according to the packaged rules 152 provided with the packaged data 108 and prevents the user or anyone else from accessing the packaged data 108 other than as allowed by the packaged rules 152. *See Schneck, col. 15, lines 20-29.* Figure 9 is an alternative embodiment of the access mechanism 114. *See Schneck, col. 16, lines 27-38.* Figure 10(a) merely illustrates the accessing operation performed by the access mechanism 114. *See Schneck, col. 17, lines 34-41.* Figure 10(b) merely illustrates a process of writing data that has already been accessed. *See Schneck, col. 20, lines 39-49.* Figures 11, 12 and 13 also merely illustrate the access operation performed by the access mechanism. *See Schneck, col. 19, line 46-col. 20, line 38.* Figures 13 and 14 merely illustrate what the access mechanism 114 performs when tampering is detected. *See*

Schneck, col. 21, lines 35-46. Finally, Figure 15 is an alternative embodiment of the information distribution system. *Compare with Figure 1.*

It is noted that none of the relied upon Figures and the corresponding description of *Schneck* teaches or suggests any type of “generating a key data using at least a unique ID of the digital data playing device or the storage medium” and “encrypting within the source device the digital data file using said key data” as recited in claim 1. Indeed, as demonstrated in previous replies, *Schneck* specifically states “that data-encrypting key, K_D , is the same for all copies of the data.” See *Schneck*, col. 12, lines 4-5. This specifically teaches away from generating an encrypting key that is based on a unique ID of the digital data playing device or the storage medium, as required by claims 1 and 47.

Further, the rule encrypting key K_R of *Schneck* cannot be equivalent to the key data as recited since *Schneck* clearly states that only the data encrypting key K_D is used to encrypt the data, not the rule encrypting key K_R . Neither Ishiguro nor the conventional art is relied upon to correct for at least this deficiency of *Schneck*. This alone is sufficient to distinguish independent claims 1 and 47 from the combination of *Schneck*, Ishiguro and the conventional art.

Claims 1 and 47 are also distinguishable for the following reason. The Examiner admits that *Scheck* does not disclose the features of “transmitting

said key data from the digital data playing device to a unit of the source device through a network" and "a decoding unit configured to decrypt the digital data file read from the data storage medium using said key data," as recited in claims 1 and 47. But the Examiner alleges that Ishiguro teaches these features. The Examiner alleges that the DVD player as disclosed in Ishiguro is equivalent to the playing device and that the computer is equivalent to the source device as claimed. The Examiner also alleges that Ishiguro teaches that the DVD player generates and transmits a key to the computer that encrypts data contact in using the transmitted key.

However, the Examiner misapplies the teachings of Ishiguro. Ishiguro actually teaches the following. As illustrated in Figure 4 and the related description, the DVD player of Ishiguro merely includes a service key and a hash function. But neither the service key nor the hash function is particular to the DVD player. Therefore, it is impossible for the DVD player to generate an encryption key based on the unique ID of itself.

Indeed, step S1 of Figure 4 in Ishiguro clearly indicates that the DVD player requests the ID information of the personal computer. Based on the ID information provided by the personal computer, the DVD player generates a source side common session key S_k in step S6. Then, the source side common session key - S_k generated in step S6 is encrypted and passed through the computer in step S7.

It is clear that the common source key S_k generated by the DVD player is based on the ID of the personal computer, and is **not** based on the unique ID of the DVD player itself. Clearly, contrary to the Examiner's allegation, Ishiguro cannot teach the feature of transmitting the key data from the digital data playing device to a unit of the source device as recited in claims 1 and 47. Indeed, Ishiguro teaches exactly the opposite.

In addition, Ishiguro does not teach that the DVD decrypts any data file from any type of storage medium. The conventional art is not relied upon to correct for any of the above noted deficiencies of Schneck and Ishiguro.

For at least the reasons stated above, it is clear that independent claims 1 and 47 are distinguishable over the combination of Schneck, Ishiguro and the conventional art.

Claims 2-3 and 48-49 depend from independent claims 1 and 47 directly or indirectly. Therefore, for at least due to the dependency thereon, claims 2-3 and 48-49 are also distinguishable over the combination of Schneck, Ishiguro and the conventional art.

Applicants respectfully request that the rejection of claims 1-3 and 47-49 based on Schneck, Ishiguro and the conventional art be withdrawn.

§ 103 REJECTION – SCHNECK, ISHIGURO, MENEZES

Claims 45-46 and 50-51 stand rejected under a combination of Schneck and Ishiguro and in further view of Menezes (Handbook of Applied Cryptography © 1997). Applicants respectfully traverse.

Claims 45 and 46 depend from independent claim 1 and claims 50 and 51 depend from independent claim 47. It has been shown above that claims 1 and 47 are distinguishable over the combination of Schneck and Ishiguro. Menezes is not relied upon to correct for the deficiencies of Schneck and Ishiguro. Therefore, independent claims 1 and 47 are distinguishable over the combination of Schneck, Ishiguro and Menezes.

For at least due to the dependency thereon, claims 45-46 and 50-51 are also distinguishable over the combination of Schneck, Ishiguro and Menezes. Applicants respectfully request that the rejection of claims 45-46 and 50-51 based on Schneck, Ishiguro and Menezes be withdrawn.

Further, Applicants respectfully challenge the Official Notice taken by the Examiner alleging that it is well known in the computer networking arts that MP3 devices are used by end users and that generation of encryption keys is accomplished by such devices. The Examiner has yet to provide a valid prior art supporting the assertions of the Official Notice. Applicants once again request that such prior art be provided.

CONCLUSION

All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the present application is in condition for allowance. Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact Hyung Sohn (Reg. No. 44,346), to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,


BIRCH, STEWART, KOLASCH &, BIRCH, LLP

By: 

Esther H. Chong, #40,953

#39,538

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000


EHC/HNS/bad